REMARKS

Upon entry of this amendment, Claims 15-47 will be pending in this application. In view of the foregoing amendments and the following remarks, applicant respectfully requests consideration of the new Claims.

New Claims 15-47 are not anticipated or made obvious by, and further differentiate the claimed invention over the prior art of record. Elements that contribute to the Claims' novelty include, but are not limited to, the following.

Claim 15 recites the delivery of the encrypt/decrypt engine via a web page, encryption independent from the identity of the client. Ross requires dependence on the identity of the physical client. In the current invention, the encryption key is derived from the user of the client and not the physical client.

Claim 16 recites that the encryption key in the current invention is entered by the user and is independent of the identity of the physical client. Because there may be the possibility to confuse the physical client identity and the user client identity, clarification has been made herein. It is quite clear from Fig. 8 that the invention has always been with respect to the user of the client and not the physical client itself.

Claim 17 recites delivery of stored data responsive to completion of a processing step.

Claim 18 recites storage of encrypted data followed by delivery of the stored data responsive to a request from either the original client or another client.

Claim 19 recites lower limits on the number of times a key must be transmitted. The crux of the invention is embodied herein, in that a de facto authentication takes place, because while the authentication information is not sent, the server can determine exactly the source of the data if and only if it can in fact decrypt the data. No prior art can be found where the authentication is tied explicitly to the ability to decrypt an encrypted text and not to a comparison of user identification tokens (username and password for example). Consequently, the shared key is only sent to the server one time and may never be sent to the client.

Laursen et al, (6,065,120) have a similar strategy, but in fact they utilize information about the user base on the client. The authentication and subsequently the encryption/decryption is tied to whether the user can identify themselves based on information that is transmitted. Additionally, they explicitly state that the invention that we have here is excluded intentionally by their invention (page 3, line 1). Our invention,

renders the username and password strong and is thus diametrically opposite to what they have invented.

Bodnar (6,061,790) proposes a system wherein two different keys are required for logging in and transmitting data. Additionally, Bodnar requires the client (page 10, last paragraph) to make use of client hardware to generate the encryption key. It would not be a trivial exercise to get our invention from this patent. Again. Bodner is concerned only with the transmission of ones own transmissions. We are of the opinion that it would be impossible to utilize Bodnar to send and receive email without the use of public/private key pairs that would need to be distribute. Also, it is clear from both Bodner and Ross, that identifying information on the server is used to authenticate and thus initiate the session (Bodner page 10 line 10, for example)

Claim 22 recites an encrypt/decrypt engine configured to operated independently of the identity of the client.

Claim 23 recites decryption and re-encryption of the data using a key of the server.

Claim 24 recites encryption of data for delivery responsive to the completion of a processing step. The encryption using the shared key or another shared key. Delivery may be to the client or another client.

Claim 25 is similar to Claim 24 except that operation is responsive to a request for the data.

Claims 25 and 26 include two possibilities for the source of a request for data.

Claim 28 recites the restriction of storage, of all data entered by the user on the client, to storage in encrypted form. Claim 28 also recites use of a key entered by the user for encryption.

Claim 29 recites use of a symmetric key.

Claim 31 is a method claim reciting use of a web page to deliver the encrypt/decrypt engine and reciting use of a shared key entered by a user.

Claims 32-36 include various methods of processing the data receive at the server.

Claims 37-41 recites a computer-readable medium comprising program instructions. The program instructions may execute methods of the invention possibly using the systems of the invention.

Claim 42 is a method claim including encryption of data independently of an identity of the client using a shared key entered by a user. Here it must be explicitly understood that the client is the device that

communicates with a server, whereas, the user is the actual entity causing the client to perform work. Claim 42 adds considerable new novelty because the user is not tied to a specific client and, the authentication and data delivery is tied to the user and not the physical client.

Claim 43-47 include further details of the step of processing data decrypted at the server.

Conclusion

In specifying the invention, the Applicant has reviewed the prior art of Krajewski (5,590,199), Linehan (5,495,533), Diffie et al (5,371,794), Wobber et al (5,235,642), Lennon et al (4,193,131), Barnes et al (5,970,475), Smithies et,al (6,091,835), Ross (5,812,671) and others. None of these would preclude the current invention from being allowed.

The Applicant respectfully request a Notice of Allowability. If the Examiner has questions regarding the case, the Examiner is invited to contact Applicant's undersigned representative at the number given below.

Dated: September 27, 2002 By: _____

Lynn D. SPraggs, Ph.D.
Ultra Information Systems Inc.
2179 11th Ave.
Vernon, BC Canada V1T 8V7
Tel: (250) 542-0112
Fax: (250) 549-3751
e-mail: lspraggs@uisamerica.com

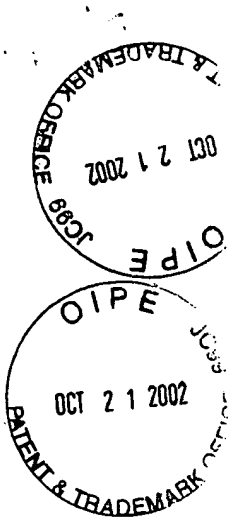
Appendix showing changes to the Specification.

On page 6 starting at line 14:

Referring now to FIG. 1, a schematic diagram illustrates a server 100 used to receive encrypted data from a sending client computer 102 and transmit encrypted data to a receiving client computer 104 through the Internet 106 using shared private keys. The sending client 102 and receiving client 104 share their own private key with the server 100, but do not share their private keys with anyone else.

On page 8 starting at line 6:

FIG. 5 is a block diagram of one embodiment of the non-volatile memory module 406 located within the clients 102, 104 of FIG. 4. The non-volatile memory 406 includes an encrypt/decrypt engine 502 for encrypting and decrypting data. The encrypt/decrypt engine 502 can also be stored in RAM 404. Excellent results can be obtained when the encrypt/decrypt engine is served up as a Java™ applet to the clients 102, 104. The Java™ applet can be served up with a web page from an email sent to the clients 102, 104, and then stored on their hard drive.



MARKED UP COPY

FOR INFORMATION PURPOSES ONLY

PLEASE DESTROY AFTER USING

APPLICANT:	Lynn D. Spraggs.
SERIAL NO.:	09/554,419
FILING DATE:	May 11, 2000
TITLE:	SYSTEM AND METHOD OF SENDING AND RECEIVING SECURE DATA WITH A SHARED KEY
EXAMINER:	Matthew B. Smithers
ART UNIT:	2132
ATTY. DKT. NO:	PA1065US

IN THE

UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANT:	Lynn D. Spraggs.
SERIAL NO.:	09/554,419
FILING DATE:	May 11, 2000
TITLE:	SYSTEM AND METHOD OF SENDING AND RECEIVING SECURE DATA WITH A SHARED KEY
EXAMINER:	Matthew B. Smithers
ART UNIT:	2132
ATTY. DKT. NO:	PA1065US

CERTIFICATE OF MAILING

I hereby certify that this paper is being deposited with the ~~United States~~Canadian Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, Washington, D.C. 20231, on the date printed below:

Date: ~~April~~ October 2, 2002

~~Steven M. Colby~~Lynn D. Spraggs

COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

AMENDMENT

Sir:

In response to the Office Action mailed ~~October~~ July 3~~2~~, ~~2001~~ 2002 (paper #~~5~~8), please amend the above-identified application as follows.

NOTE: 1. With respect to objection of Claims 44 –47 we have redone them to be dependent on claim 43 instead of claim 42.

NOTE: 2. With respect to objection of claims 15-30 and 38 –47 we have made reference in both the amended claims and the remarks.

NOTE: 3. With respect to Both Laursen and Bodner, reference to these is given in the remarks. It is to be noted that there must be some overlap because of the nature of computer systems and computer software, but taken in the context of this application, the invention is both novel and innovative and cannot be inferred from other prior art.

NOTE: 4. We are returning the new document along with a marked up version so you can easily determine the differences.

In the Specification:

Replace the paragraph beginning on page 6 line 14 with:

> Referring now to FIG. 1, a schematic diagram illustrates a server 100 used to receive encrypted data from a sending client computer 102 and transmit encrypted data to a receiving client computer 104 through the Internet 106 using shared private keys. The sending client 102 and receiving client 104 share their own private key with the server 100, but do not share their private key with anyone else.

Replace the paragraph beginning on page 8 line 6 with:

FIG. 5 is a block diagram of one embodiment of the non-volatile memory module 404 located within the clients 102, 104 of FIG. 4. The non-volatile memory 406 includes an encrypt/decrypt engine 502 for encrypting and decrypting data. The encrypt/decrypt engine 502 can also be stored in RAM 404. Excellent results can be obtained when the encrypt/decrypt engine is served up as a Java™ applet to the clients 102, 104. The Java™ applet can be served up with a web page. In another form, the encrypt/decrypt engine can be ~~from an email~~ sent to the clients 102, 104, and then stored on their hard drive.

In the Claims:

Cancel Claims 1-14 and add the following new Claims 15-47.

15. (New) A system for using a shared key to transmit secure data between a client and a server, the system comprising:

an encrypt/decrypt engine for using the shared key to encrypt or decrypt data, the encrypt/decrypt engine being configured for delivery via a web page to a client in response to a user request and further configured to encrypt data independently of an identity of the physical client;

wherein the server includes a user private keys database configured to store the shared key. And, wherein, it is possible for the client and the server to reside on the same physical computing device.

16. (New) The system of claim 15 wherein the shared key is a user's private key entered by a user into the web page.

17. (New) The system of claim 15 further comprising a secure data database configured to store data received from the client and, upon the completion of a processing step, to deliver the stored data in an encrypted format to the client or to another client.

18. (New) The system of claim 15 further comprising a secure data database configured to store data received from the client and,

upon receipt of a request for the data, to deliver the stored data in an encrypted format to the client or to another client.

19. (New) The system of claim 15 wherein the shared key is transmitted between the server and the client as few as zero times and the shared key is transmitted between the server and the user as few as one time. The key is not sent for authentication purposes, rather, the effect of the key in the encryption process is sent. Consequently, the shared key does not need to be retransmitted once it has been established.

20. (New) The system of claim 15 wherein the shared key is a user's private key entered by a user.

21. (New) The system of claim 15 wherein the client encrypt/decrypt engine is installed on the client.

22. (New) A system for using a shared key in transmitting secure data between a client and a server, the system comprising:

an encrypt/decrypt engine for using the shared key in encrypting data, the encrypt/decrypt engine being configured to encrypt data independently of an identity of the client; and

a user private keys database located on the server and configured to store the shared key, the shared key being the private key of a user.

23. (New) The system of claim 22 wherein the server is configured to decrypt encrypted data received from the client using the shared key and to use a private server key, known only by the server, to re-encrypt the decrypted data.

24. (New) The system of claim 23 further comprising a secure data database configured to store the encrypted data received from the client and re-encrypted by the server and to deliver the stored data to the client or to another client; the delivered data, after the completion of a processing step, being encrypted with the shared user key or with another shared user key.

25. (New) The system of claim 23 further comprising a secure data database configured to store the encrypted data received from the client and re-encrypted by the server and to deliver the stored data to the client or to another client; the delivered data being, upon receipt of a request for the data, encrypted with the shared user key or with another shared user key.

26. (New) The system of claim 25 wherein the request is from the user.

27. (New) The system of claim 25 wherein the request is from an other user.

28. (New) A system for using a shared key in transmitting secure data between a client and a server, the system comprising:

an encrypt/decrypt engine for using the shared key entered by a user to encrypt data entered by the user, the encrypt/decrypt engine being configured such that all data entered by the user and stored on the client is stored in encrypted form, and further configured to encrypt data independently of an identity of the physical client; the shared key entry being the responsibility of the user and not the client;

the server including a user private keys database configured to store the shared key, the shared key being a private key of a user; and not a physical client

29. (New) The system of claim 28, wherein the encrypt/decrypt engine uses a symmetric key encryption/decryption algorithm for encrypting and decrypting data.

30. (New) The system of claim 28, further including a web server engine configured for the user to securely send or receive data from the client to the server.

31. (New) A method for using a shared key in receiving secure data on a server, comprising the steps of:

delivering from a server to a client a web page including an encrypt/decrypt engine;

encrypting data on the client using the encrypt/decrypt engine and a shared key entered by a user of the client, the shared key being shared between the user and the server;

delivering the encrypted data from the client to the server;

receiving the encrypted data at the server;

decrypting the encrypted data at the server using the shared key; and

processing the decrypted data.

32. (New) The method of claim 31, wherein the step of processing the decrypted data includes the steps of:

encrypting the decrypted data with a private server key; and

storing the encrypted data in a database.

33. (New) The method of claim 31, wherein the step of processing the decrypted data includes the steps of:

re-encrypting the data with an other user's private key shared between the other user and the server; and

sending the re-encrypted data to the other user.

34. (New) The method of claim 31, wherein the step of processing the decrypted data includes the steps of:

decrypting the encrypted data with the private server key;

re-encrypting the data with a second user's key shared between the second user and the server; and

sending the re-encrypted data to the second user.

35. (New) The method of claim 31, wherein the step of processing the decrypted data includes the steps of:

processing the data according to an instruction of the user;

re-encrypting the processed data using the user's shared key; and

sending the re-encrypted processed data to the user.

36. (New) The method of claim 31, wherein the step of processing the decrypted data includes storing the decrypted data in a secure database.

37. (New) A computer-readable medium comprising program instructions for causing a computer system to use a shared key in receiving secure data at a server, by the steps of:

delivering a web page from the server to a client, the web page including an encrypt/decrypt engine and being configured to use the encrypt/decrypt engine and a shared key entered by a user of the client to encrypt data on the client, the shared key being shared between the user and the server;

receiving the encrypted data at the server;

decrypting the encrypted data using the shared key; and

processing the decrypted data.

38. (New) A computer-readable medium comprising program instructions for causing a computer system to receive secure data on a server using a shared key, by the steps of:

delivering an encrypt/decrypt engine from the server to a client, the encrypt/decrypt engine being configured to use a shared key entered by a user of the client to encrypt data on the client, the shared key being shared between the user and the server and the encryption being independent of an identity of the physical client;

receiving the encrypted data at the server;

decrypting the encrypted data using the shared key; and

processing the decrypted data.

39. (New) The computer readable medium of claim 38, further comprising program instructions for causing the processed decrypted data to be re-encrypted using a private server key.

40. (New) The computer-readable medium of claim 39, further comprising program instructions for causing the processed decrypted data to be stored in a secure database.

41. (New) The computer-readable medium of claim 38, wherein processing the decrypted data includes the steps of:

re-encrypting the data with the private server key;

storing the re-encrypted data;

decrypting the stored data with the private server key;

encrypting the data with a second user's key shared between the second user and the server; and

sending the encrypted data to the second user.

42. (New) The computer-readable medium of claim 38, wherein processing the decrypted data includes the steps of:

processing the data according to an instruction of the user;

encrypting the processed data using a shared key; and

sending the encrypted processed data to the user or to another user.

43. (New) A method of using a shared key in transmitting secure data between a client and a server using a shared key, comprising the steps of:

encrypting data using the shared key with an encrypt/decrypt engine configured to encrypt data independently of an identity of the client, the shared key being entered by a user of the client;

delivering the encrypted data from the client to the server;

receiving the encrypted data at the server;

decrypting the encrypted data at the server using the shared key, the shared key being stored in a user private keys database; and

processing the decrypted data.

44. (New) The method of claim ~~42~~43, wherein processing the decrypted data includes the steps of:

encrypting the decrypted data with a private server key; and

storing the encrypted data in a database.

45. (New) The method of claim ~~42~~43, wherein the step of processing the decrypted data includes the steps of:

encrypting the data with an other user's private key shared between the other user and the server; and

sending the encrypted data to the other user.

46. (New) The method of claim ~~42~~43, wherein the step of processing the decrypted data includes the steps of:

decrypting the re-encrypted data with the private server key;

encrypting the data with a second user's key shared between the second user and the server; and

sending the encrypted data to the second user.

47. (New) The method of claim ~~42~~43, wherein the step of processing the decrypted data includes the steps of:

processing the data according to an instruction of the user;

re-encrypting the processed data using the user's shared key; and

sending the re-encrypted processed data to the user.

REMARKS

Upon entry of this amendment, Claims 15-47 will be pending in this application. In view of the foregoing amendments and the following remarks, applicant respectfully requests consideration of the new Claims.

New Claims 15-47 are not anticipated or made obvious by, and further differentiate the claimed invention over the prior art of record. Elements that contribute to the Claims' novelty include, but are not limited to, the following.

Claim 15 recites the delivery of the encrypt/decrypt engine via a web page, encryption independent from the identity of the client. Ross requires dependence on the identity of the physical client. In the current invention, the encryption key is derived from the user of the client and not the physical client.

Claim 16 recites that the encryption key in the current invention is entered by the user and is independent of the identity of the physical client. Because there may be the possibility to confuse the physical client identity and the user client identity, clarification has been made herein. It is quite clear from Fig. 8 that the invention has always been with respect to the user of the client and not the physical client itself.

Claim 17 recites delivery of stored data responsive to completion of a processing step.

Claim 18 recites storage of encrypted data followed by delivery of the stored data responsive to a request from either the original client or another client.

Claim 19 recites lower limits on the number of times a key must be transmitted. The crux of the invention is embodied herein, in that a de facto authentication takes place, because while the authentication information is not sent, the server can determine exactly the source of the data if and only if it can in fact decrypt the data. No prior art can be found where the authentication is tied explicitly to the ability to decrypt an encrypted text and not to a comparison of user identification tokens (username and password for example). Consequently, the shared key is only sent to the server one time and may never be sent to the client.

Laursen et al, (6,065,120) have a similar strategy, but in fact they utilize information about the user base on the client. The authentication and subsequently the encryption/decryption is tied to whether the user can identify themselves based on information that is transmitted. Additionally, they explicitly state that the invention that we have here is excluded intentionally by their invention (page 3, line 1). Our invention,

renders the username and password strong and is thus diametrically opposite to what they have invented.

Bodnar (6,061,790) proposes a system wherein two different keys are required for logging in and transmitting data. Additionally, Bodnar requires the client (page 10, last paragraph) to make use of client hardware to generate the encryption key. It would not be a trivial exercise to get our invention from this patent. Again, Bodner is concerned only with the transmission of ones own transmissions. We are of the opinion that it would be impossible to utilize Bodnar to send and receive email without the use of public/private key pairs that would need to be distribute. Also, it is clear from both Bodner and Ross, that identifying information on the server is used to authenticate and thus initiate the session (Bodner page 10 line 10, for example)

Claim 22 recites an encrypt/decrypt engine configured to operated independently of the identity of the client.

Claim 23 recites decryption and re-encryption of the data using a key of the server.

Claim 24 recites encryption of data for delivery responsive to the completion of a processing step. The encryption using the shared key or another shared key. Delivery may be to the client or another client.

Claim 25 is similar to Claim 24 except that operation is responsive to a request for the data.

Claims 25 and 26 include two possibilities for the source of a request for data.

Claim 28 recites the restriction of storage, of all data entered by the user on the client, to storage in encrypted form. Claim 28 also recites use of a key entered by the user for encryption.

Claim 29 recites use of a symmetric key.

Claim 31 is a method claim reciting use of a web page to deliver the encrypt/decrypt engine and reciting use of a shared key entered by a user.

Claims 32-36 include various methods of processing the data receive at the server.

Claims 37-41 recites a computer-readable medium comprising program instructions. The program instructions may execute methods of the invention possibly using the systems of the invention.

Claim 42 is a method claim including encryption of data independently of an identity of the client using a shared key entered by a user. Here it must be explicitly understood that the client is the device that

communicates with a server, whereas, the user is the actual entity causing the client to perform work. Claim 42 adds considerable new novelty because the user is not tied to a specific client and, the authentication and data delivery is tied to the user and not the physical client.

Claim 43-~~46~~-47 include further details of the step of processing data decrypted at the server.

Conclusion

In specifying the invention, the Applicant has reviewed the prior art of Krajewski (5,590,199), Linehan (5,495,533), Diffie et al (5,371,794), Wobber et al (5,235,642), Lennon et al (4,193,131), Barnes et al (5,970,475), Smithies et,al (6,091,835), Ross (5,812,671) and others. None of these would preclude the current invention from being allowed.

The Applicant respectfully request a Notice of Allowability. If the Examiner has questions regarding the case, the Examiner is invited to contact Applicant's undersigned representative at the number given below.

Dated: September 27, 2002 By: _____

~~Steven M. Colby~~Lynn D. SPraggs, Ph.D.
~~Reg. No. 50,250~~
~~Carr & Ferrell, LLP~~Ultra Information Systems Inc.
~~2225 E. Bayshore Road, Suite 200~~2179 11th Ave.
~~Palo Alto~~Vernon, ~~CA~~ BC ~~94303~~Canada V1T 8V7
Tel: (~~650~~250) ~~812-3424~~542-0112
Fax: (~~650~~250) ~~812-3444~~549-3751
e-mail: ~~scolby@carr-ferrell.com~~lspraggs@uisamerica.com

Appendix showing changes to the Specification.

On page 6 starting at line 14:

Referring now to FIG. 1, a schematic diagram illustrates a server 100 used to receive encrypted data from a sending client computer 102 and transmit encrypted data to a receiving client computer 104 through the Internet 106 using shared private keys. The sending client 102 and receiving client 104 share their own private key with the server 100, but do not share their private keys with anyone else.

On page 8 starting at line 6:

FIG. 5 is a block diagram of one embodiment of the non-volatile memory module ~~404~~ 406 located within the clients 102, 104 of FIG. 4. The non-volatile memory 406 includes an encrypt/decrypt engine 502 for encrypting and decrypting data. The encrypt/decrypt engine 502 can also be stored in RAM 404. Excellent results can be obtained when the encrypt/decrypt engine is served up as a Java™ applet to the clients 102, 104. The Java™ applet can be served up with a web page from an email sent to the clients 102, 104, and then stored on their hard drive.